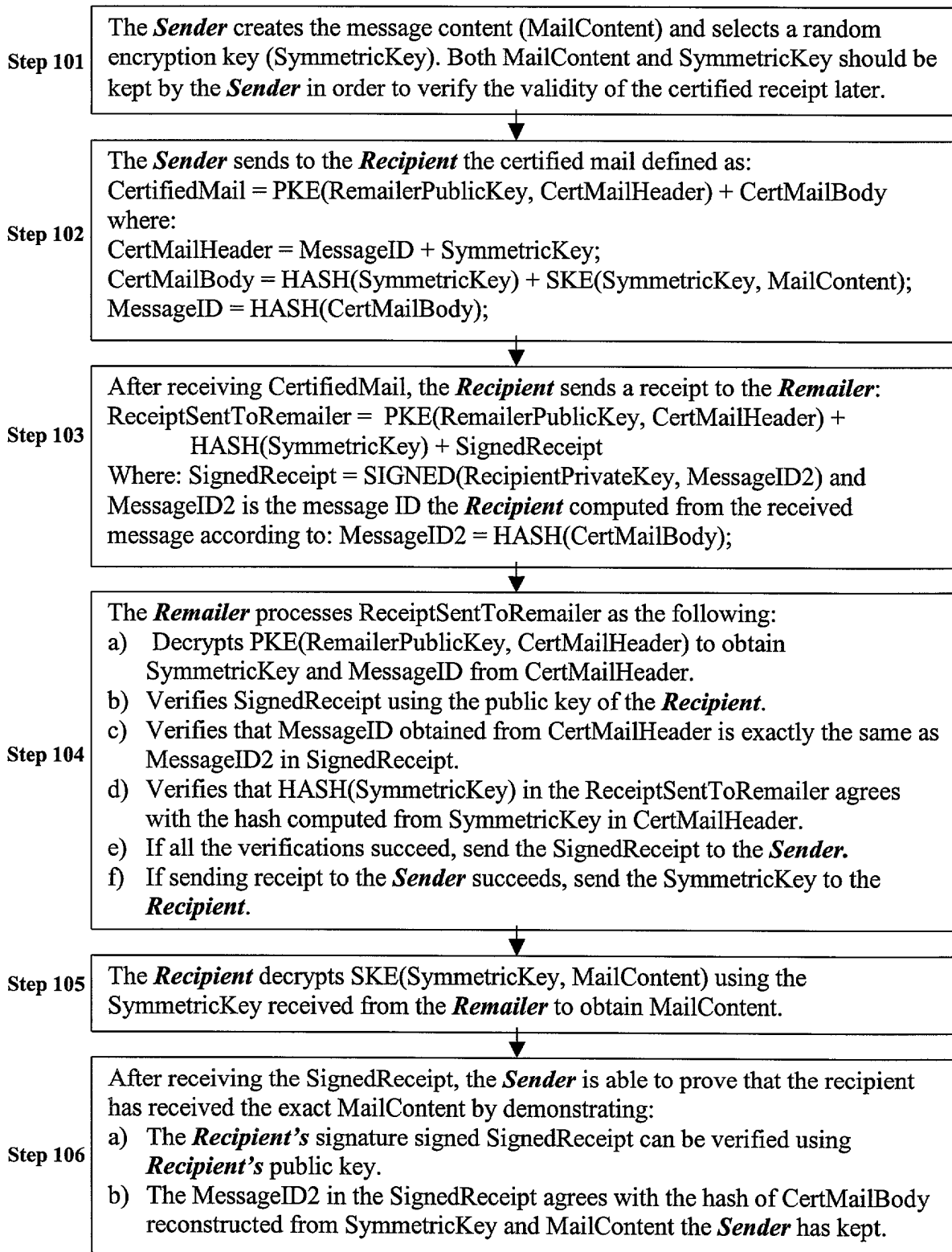
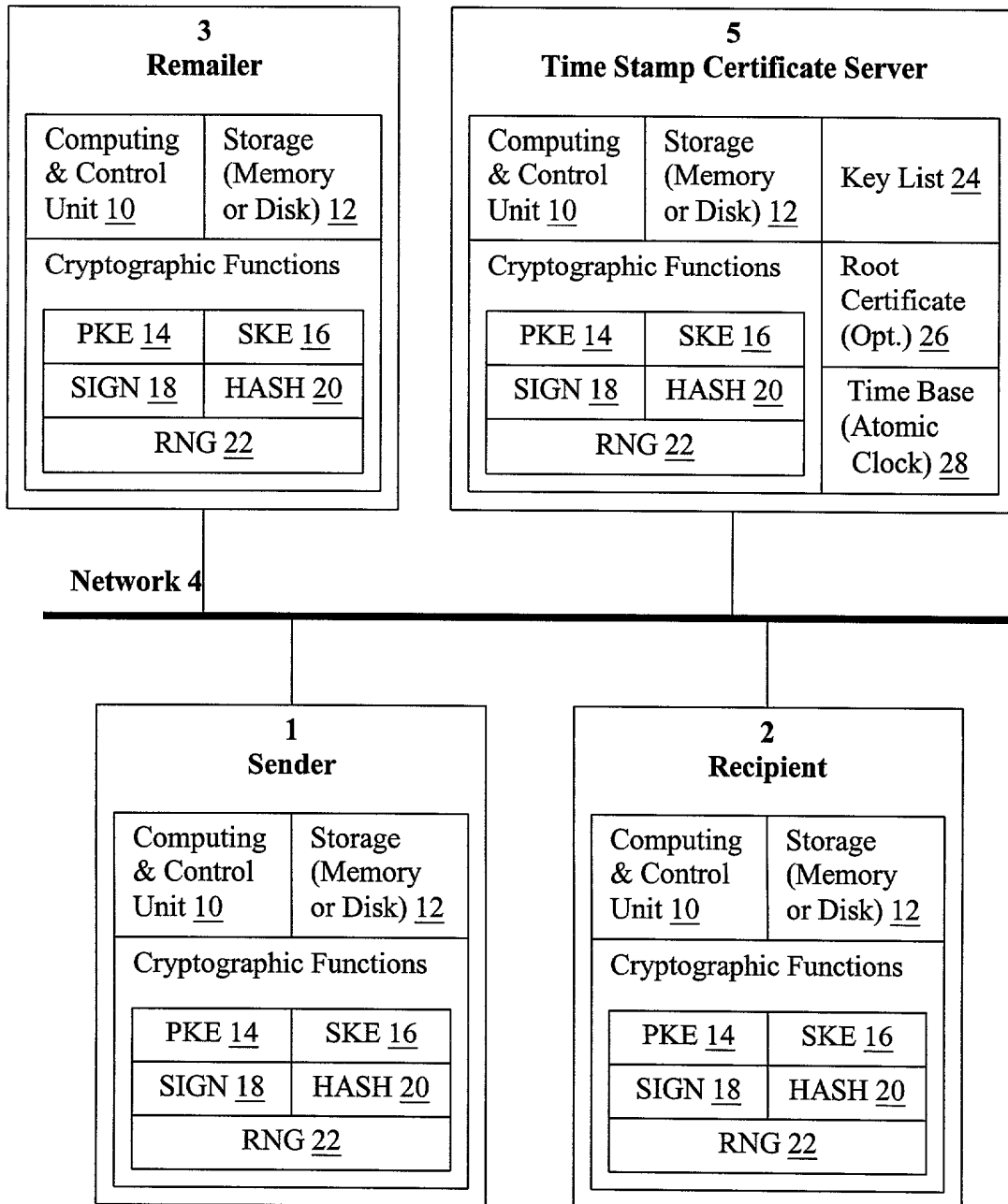


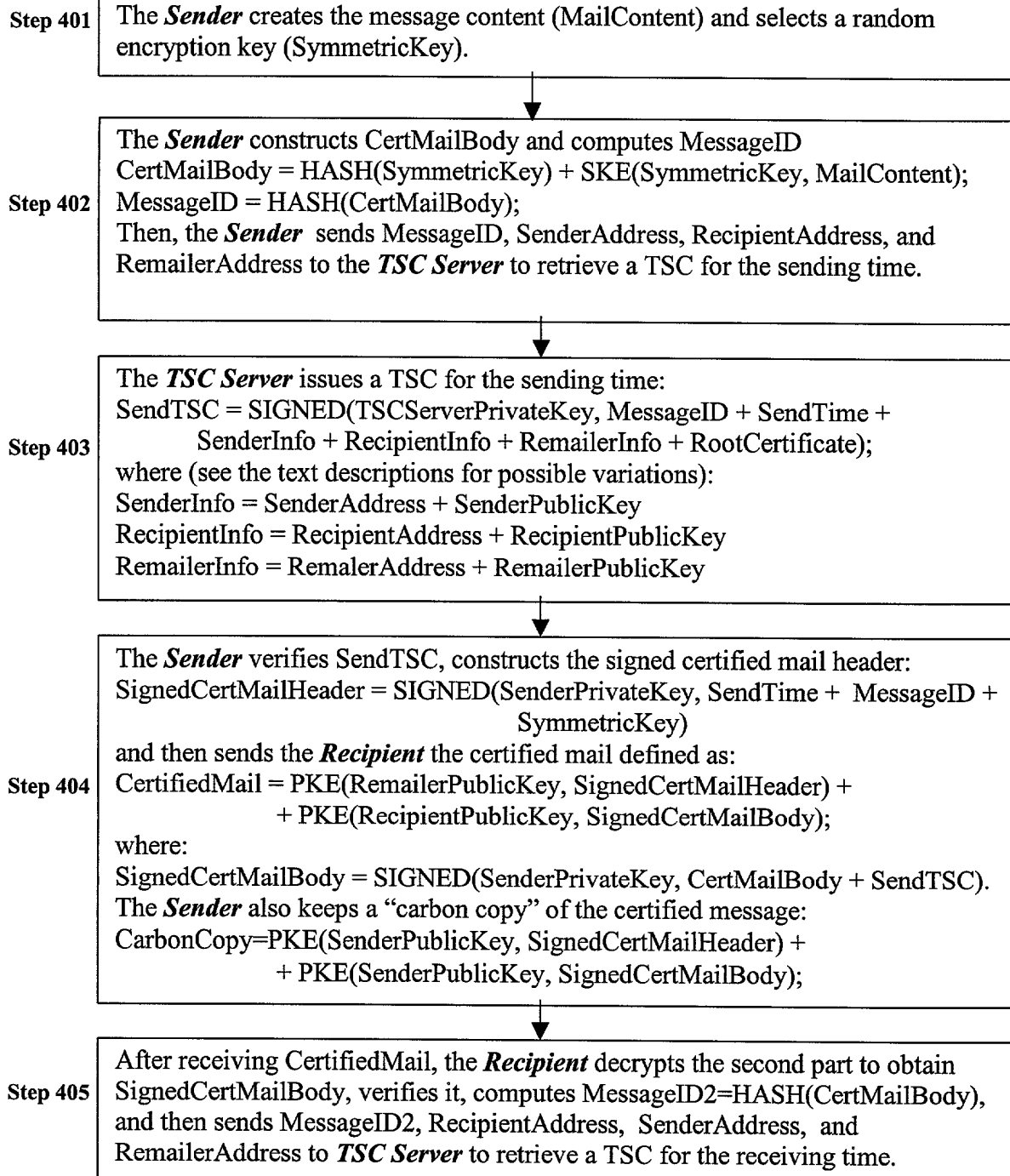
**Figure 1.**



**Figure 2**



**Figure 3.**



Continued to Figure 4b

Figure 4a

Continued from Figure 4a

Step 406

The **TSC Server** issues a TSC for the receiving time:  
ReceiveTSC = SIGNED(TSCServerPrivateKey, MessageID2 +  
ReceiveTime + RecipientInfo + SenderInfo + RemailerInfo + RootCertificate);

Step 407

The **Recipient** verifies the ReceiveTSC and sends a receipt to the **Remailer**:  
ReceiptSentToRemailer = PKE(RemailerPublicKey, SignedCertMailHeader) +  
PKE(RemailerPublicKey, HASH(SymmetricKey) + ReturnSessionKey +  
SignedReceipt), where:  
SignedReceipt = SIGNED(RecipientPrivateKey, SendTSC + ReceiveTSC)

Step 408

The **Remailer** decrypts ReceiptSentToRemailer to obtain SignedCertMailHeader, HASH(SymmetricKey), and SignedReceipt. Then, the **Remailer** conducts a series of verification steps to ensure that the SignedCertMailHeader, SignedReceipt, SendTSC, ReceiveTSC are all valid and the data contained in them are all consistent. If all the verifications succeed, the **Remailer** sends the **Sender** CertifiedReceipt = PKE(SenderPublicKey, SignedReceipt) and sends SKE(ReturnSessionKey, SymmetricKey) to the **Recipient**.

Step 409

The **Recipient** decrypts SKE(ReturnSessionKey, SymmetricKey) received from the **Remailer** to recover SymmetricKey and then use it to decrypt SKE(SymmetricKey, MailContent) to obtain MailContent.

Step 410

After receiving the CertifiedReceipt, the **Sender** is able to prove that the MailContent existed at SendTime and is delivered to the recipient at ReceiveTime by demonstrating:

- The **Recipient's** signature in SignedReceipt can be verified using RecipientPublicKey in ReceiveTSC.
- The MessageID or MessageID2, in SignedReceipt, SendTSC, ReceiveTSC, all agrees with the hash of the CertMailBody recovered from the CarbonCopy kept by the **Sender** during Step 404 above.
- SenderInfo, RecipientInfo, RemailerInfo in both SendTSC and ReceiveTSC are all consistent.
- The signatures in SendTSC and ReceiveTSC can be verified using the **TSC Server's** public key in the RootCertificate, and the RootCertificate can be verified using the root public keys.
- SendTSC in CarbonCopy is the same as the one in the SignedReceipt.

Figure 4b